Федеральное государственное автономное образовательное учреждение высшего образования
«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
Факультет информационных технологий
Кафедра «Информационная безопасность»
Направление подготовки/ специальность: 10.05.03 Информационная безопасность автоматизированных систем

ОТЧЕТ

по проектной практике

Студент: Меркулов Григорий Сергеевич Группа: 241-371
Место прохождения практики: Московский Политех, кафедра «Информационная безопасность»

Отчет принят с оценкой _____ Дата _____
Руководитель практики: Гневшев Александр Юрьевич

Москва 2025

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

В рамках проектной практики удалось поработать над задачами, которые помогли не только закрепить уже имеющиеся знания в сфере информационных технологий, но и получить новые, особенно в области разработки и обеспечения безопасности веб-приложений. Программа практики была разделена на две части — базовую и вариативную. Каждая из них включала в себя как теоретическую подготовку, так и практическую отработку ключевых ИТ-навыков.

На первом этапе — в базовой части — основной акцент был сделан на создание статического сайта с помощью генератора Hugo. Этот сайт стал площадкой для размещения информации о текущем проекте, который реализовывался в рамках дисциплины «Проектная деятельность». Кроме того, в этот период удалось поучаствовать в мастер-классе от компании «Инфосистемы Джет» на тему «Как развиваться в ИБ». Встреча оказалась очень полезной: она дала представление о карьерных перспективах в сфере информационной безопасности и позволила лучше понять современные тренды в этой области.

Вариативная часть практики была сосредоточена на изучении методов тестирования защищенности веб-приложений. В рамках этого этапа проводился обзор актуальных подходов, инструментов и стандартов, которые применяются для выявления уязвимостей в веб-среде. Работа с этой темой позволила глубже понять принципы кибербезопасности и научиться подходить к вопросам цифровой защиты более системно.

Благодаря выполненным заданиям удалось не только развить технические навыки, но и расширить кругозор в области веб-разработки и информационной безопасности. В отчете подробно описаны все этапы практики, достигнутые результаты и ключевые выводы, сделанные по итогам работы.

1. Основная информация о проекте

1. Название проекта:

Помощь людям с ОВЗ: сайт для оказания экстренной помощи

2.Цели и задачи проекта:

Данный раздел определяет цели и задачи проекта и его исследовательской части, а также объект и предмет. Цель проекта – это конечный результат, которую команда проекта хочет достичь в ходе выполнения проекта. Исходя из целей проекта, формируются его задачи, которые существуют для того, чтобы дать наводку на действия для достижения целей. Важное уточнение: в данном контексте, задачи появляются по мере разработки, поэтому здесь задачи описаны в рамках первой аттестации. Ниже представлены такие понятия как «объект» и «предмет» проекта. Объект представляет собой изучаемое, предмет подразумевает за собой свойство изучаемого.

Объект проекта: Сайт для помощи людям с ОВЗ и инвалидам.

Предмет проекта: Разработка сайта для помощи людям с ОВЗ и инвалидам «Поддержка рядом».

Цель проекта:

- Создание сайта для взаимодействия волонтеров и лиц с ОВЗ в одном из административных округов г. Москва.

Задачи:

- Создание дизайна главных страниц.
- Разработка интерактивных элементов для главной страницы.
- Верстка сайта.
- Создание базы данных
- Создание политики конфиденциальности
- Адаптация сайта под мобильные устройства
- Запустить продвижение сайта в соцсетях
- Составление диаграммы Ганта
- Составление проектно-технической документации

- Подготовка презентации к защите проекта
- Защита проекта

2. Общая характеристика деятельности организации

1. Наименование заказчика:

Московский Политехнический университет

2. Организационная структура:

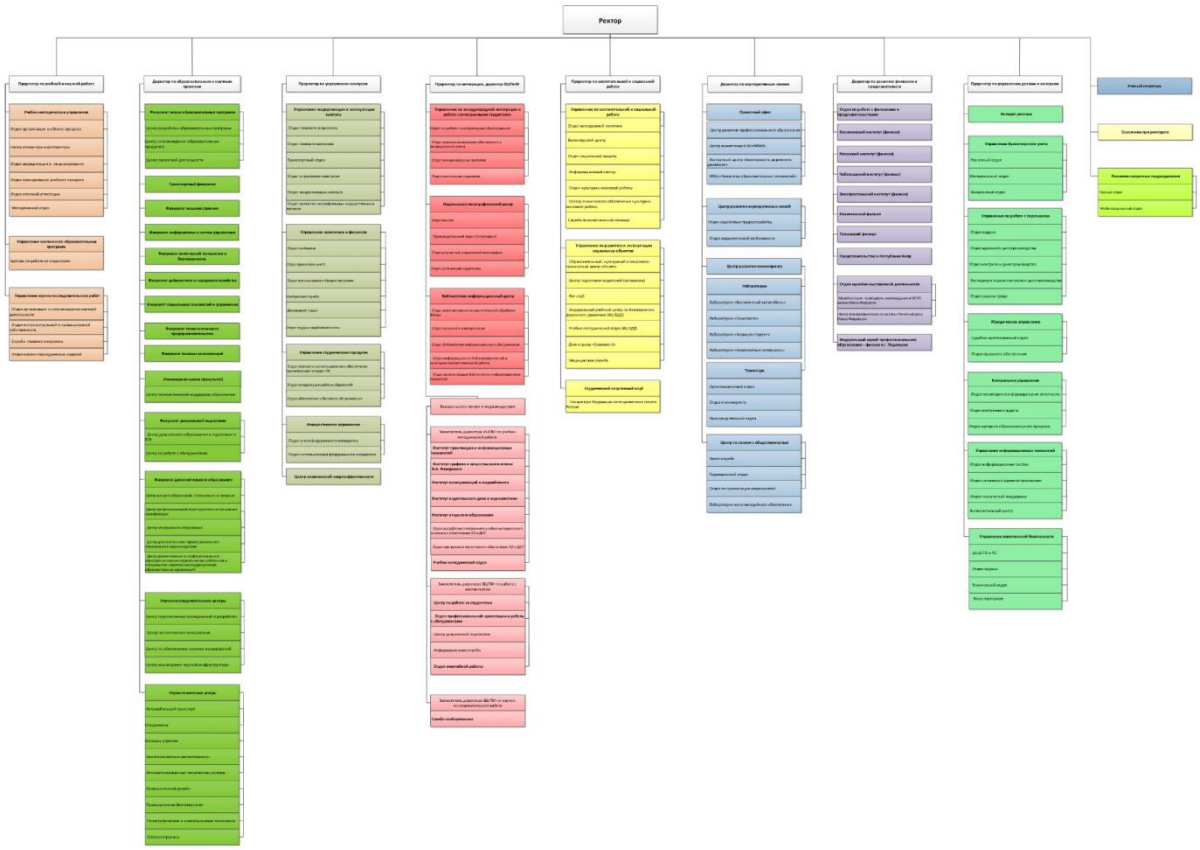

Рисунок 1 – Организационная структура организации «Московский политехнический университет»

3. Описание деятельности:

Московский политехнический университет – это ведущее образовательное и научное учреждение, сочетающее традиции академического мастерства с инновационными подходами в подготовке высококвалифицированных специалистов для высокотехнологичных отраслей экономики. Университет осуществляет многопрофильную деятельность, включающую образовательные программы бакалавриата, специалитета, магистратуры и аспирантуры по направлениям, связанным с инженерией, IT, робототехникой, энергетикой, транспортом, биотехнологиями и другими ключевыми областями современной науки и промышленности. Вуз активно

развивает прикладные исследования, сотрудничая с крупнейшими корпорациями и научными центрами, что позволяет студентам и преподавателям участвовать в реальных проектах, направленных на решение актуальных технологических и социально-экономических задач. Московский политехнический университет уделяет особое внимание интеграции образования, науки и производства, внедряя междисциплинарные подходы и современные методики обучения, включая цифровые технологии и проектно-ориентированное образование. Университет также является площадкой для развития предпринимательских инициатив, поддерживая стартапы и инновационные разработки своих студентов и сотрудников. Среди приоритетных направлений деятельности – международное сотрудничество, участие в глобальных научных и образовательных программах, а также подготовка кадров, способных конкурировать на мировом уровне. Московский политехнический университет стремится к формированию новой генерации инженеров, ученых и управленцев, готовых к вызовам быстро меняющегося технологического ландшафта.

3. Описание задания по проектной практике

1. Базовая часть задания

В ходе работы над практикой удалось освоить несколько полезных инструментов, которые существенно упростили процесс создания веб-сайта. В частности, изучение основ работы с системой контроля версий Git дало возможность лучше организовать работу над проектом и отслеживать изменения. Также был изучен язык разметки Markdown, что помогло эффективно оформлять текстовый контент для сайта.

Особое внимание было уделено освоению генератора статических сайтов Hugo. Этот инструмент оказался удобным и функциональным — благодаря ему удалось быстрее и проще собрать структуру сайта. Сам сайт был посвящён проекту, выполняемому в рамках дисциплины «Проектная деятельность», и включал несколько ключевых разделов: «О проекте» (с описанием целей, задач и актуальности), «Участники» (с информацией о членах команды), «Журнал» (где публиковались отчёты о ходе выполнения работы) и «Ресурсы» (с полезными ссылками на материалы по теме). Создание сайта стало важным шагом в понимании веб-разработки на практике.

Значимой частью практики стало участие в мастер-классе, организованном компанией «Инфосистемы Джет» на тему «Как развиваться в ИБ». В рамках занятия участники моделировали построение защищённой информационной системы, оперируя ограниченным бюджетом в 200 джеткоинов. Предлагалось выбирать меры защиты из трёх направлений: технические решения, организационные подходы и персонал. Каждая из них имела свою стоимость и оценивалась по уровню защищённости. Работа над заданием включала анализ доступных вариантов, сравнение их эффективности, определение приоритетов и формирование финальной конфигурации системы. В ходе выполнения задачи удалось прийти к интересному выводу: для небольших компаний зачастую выгоднее инвестировать в квалифицированный персонал, чем в дорогостоящее

программное обеспечение. Грамотно подобранные специалисты могут обеспечить гибкую и устойчивую защиту при меньших затратах.

В результате всей практики были получены ценные навыки работы с современными инструментами разработки, укреплены принципы командного взаимодействия и налажено первое профессиональное общение с ИТ-сообществом. Все поставленные задачи были успешно выполнены в срок и в полном объеме.

2. Вариативная часть

Индивидуальное задание разработано с целью развития профессиональных компетенций, соответствующих направлению «Информационная безопасность автоматизированных систем»

Тема: «Анализ методик тестирования защищенности веб-приложений»

Поставленные задачи:

1. Классифицировать методы тестирования защищенности веб-приложений.
2. Рассмотреть основные уязвимости и методы их выявления.
3. Сравнить инструменты и подходы к тестированию.
4. Проанализировать методологии и стандарты тестирования (OWASP, PTES, NIST, ISO).
5. Изучить практические аспекты тестирования, включая этапы, особенности API-тестирования и юридические аспекты.
6. Оценить эффективность различных методик (автоматизированные vs ручные, ложные срабатывания, метрики безопасности).
7. Разработать рекомендации по выбору подходов в зависимости от типа приложения, ресурсов команды и регуляторных требований.

4. Описание достигнутых результатов по проектной практике

В ходе выполнения **базовой части** мной были достигнуты следующие результаты:

1. Были изучены базовые команды и принципы работы с системой контроля версий Git. Выполнены первичные коммиты, созданы ветки. **Затраченное время: 9 часа**

2. Был изучен синтаксис языка разметки Markdown. На его основе оформлены документы в репозитории, а также созданы и наполнены содержанием основные разделы сайта. **Затраченное время: 7 часов**

3. Были изучены ключевые функции генератора статических сайтов Hugo. С его помощью был создан и запущен сайт, определена его структура, добавлены и оформлены разделы «Участники» и «Журнал». З**атраченное время: 22 часов**

4. Было посещено мероприятие организации-партнера от компании «Инфосистемы Джет» на тему «Как развиваться в ИБ». **Затраченное время: 2 часа**

В ходе выполнения **вариативной части** мной были достигнуты следующие результаты:

В процессе выполнения вариативной части практики, посвящённой тестированию защищённости веб-приложений, удалось успешно справиться со всеми поставленными задачами и достичь запланированных результатов:

1. Классификация методов тестирования защищённости Были изучены основные подходы к тестированию безопасности веб-приложений: статический анализ (SAST), динамический (DAST), интерактивный (IAST), ручное тестирование и автоматизированное сканирование. Проанализированы сильные и слабые стороны каждого метода, а также их применимость на разных этапах жизненного цикла разработки. Сформированы критерии выбора подхода в зависимости от целей проекта и специфики среды. **Затраченное время: 10 часов**

2. Сравнение инструментов и подходов к тестированию Проведён обзор ряда популярных инструментов, включая Burp Suite, OWASP ZAP, SQLmap, Metasploit, SonarQube и Dependency-Check. Были рассмотрены их возможности, эффективность в выявлении уязвимостей и удобство интеграции в процессы CI/CD. На основе анализа определены подходящие комбинации для разных задач — от пентестов до аудитов безопасности. **Затраченное время: 12 часов**

3. Изучение практических аспектов тестирования Подробно изучены этапы проведения тестирования: от планирования и сбора информации до эксплуатации уязвимостей и составления отчетов. Особое внимание было уделено безопасности API (в том числе REST и GraphQL), а также правовым и этическим аспектам тестирования — таким как соблюдение законодательства и политика ответственного раскрытия уязвимостей. **Затраченное время: 10 часов**

ЗАКЛЮЧЕНИЕ

Все задачи, поставленные в рамках как базовой, так и вариативной части практики, были успешно реализованы. В процессе работы были освоены важные навыки: использование системы Git, разработка и публикация сайта с помощью Hugo, участие в карьерном марафоне, а также оформление технической документации в профессиональном формате. Особенно полезным оказался практический кейс от компании «Инфосистемы Джет», в рамках которого удалось применить стратегический подход к созданию системы ИБ при ограниченных ресурсах.

Центральным результатом практики стало проведение углублённого анализа в трёх ключевых направлениях: классификация методов тестирования защищённости веб-приложений, сравнение современных инструментов и подходов, а также изучение практических аспектов проведения тестирования. Были изучены и систематизированы подходы SAST, DAST, IAST, а также ручное и автоматизированное тестирование, определены их преимущества, ограничения и области применения. Проведён обзор инструментов — от Burp Suite и OWASP ZAP до SonarQube и Metasploit — с акцентом на их функциональность и интеграцию в процессы разработки. Особое внимание было уделено практическим этапам тестирования, включая планирование, сканирование, эксплуатацию уязвимостей, работу с API и правовые аспекты.

Полученные выводы подтвердили важность комплексного подхода, сочетающего технические средства с экспертной оценкой для обеспечения надёжной информационной безопасности.

Полученные знания и практический опыт стали прочной базой для дальнейшего развития в сфере информационной безопасности и будущей проектной деятельности.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. OWASP Web security testing guide // Owasp URL: https://owasp.org/www-project-web-security-testing-guide/ (дата обращения: 10.05.2025).
2. SP 800-115, Technical Guide to Information Security Testing and Assessment // Nist URL: https://csrc.nist.gov/pubs/sp/800/115/final (дата обращения: 10.05.2025).
3. The Penetration Testing Execution Standart // Pentest-standart URL: http://www.pentest-standard.org/index.php/Main_Page (дата обращения: 10.05.2025).
4. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements. – Международный стандарт. – 2022. – 44 с.
5. ISO/IEC 27034-1:2011 Information technology — Security techniques — Application security — Part 1: Overview and concepts. – Международный стандарт. – 2011. – 32 с.
6. ГОСТ Р 7.0.100-2018. Библиографическая запись. Библиографическое описание. Общие требования и правила составления : национальный стандарт Российской Федерации. – Введ. 2019-07-01. – Москва : Стандартинформ, 2018. – 124 с.
7. Hugo Static Site Generator : [сайт]. – URL: https://gohugo.io (дата обращения: 15.05.2025).